# Separably closed fields with Hasse derivations

Martin Ziegler

September 11, 2002

#### Abstract

In [6] Messmer and Wood proved quantifier elimination for separably closed fields of finite Ershov invariant e equipped with a (certain) Hasse derivation. We propose a variant of their theory, using a sequence of e commuting Hasse derivations. In contrast to [6] our Hasse derivations are iterative.

## 1 Introduction

**Definition.** Let R be a commutative ring. A Hasse derivation is a family  $D = (D_0, D_1, \ldots)$  of additive maps  $D_n : R \to R$  such that<sup>1</sup>

$$D_0(x) = x \tag{1.1}$$

$$D_n(xy) = \sum_{a+b=n} D_a(x)D_b(y) \tag{1.2}$$

$$D_a D_b = \binom{a+b}{a} D_{a+b} \quad . \tag{1.3}$$

Two Hasse derivations D and E commute if  $D_m E_n = E_n D_m$  for all m, n.

We fix for the rest of the paper a natural number e and a prime p.

The following notion was introduced by Okugawa in [7]: A  $\mathcal{D}$ -field is a pair  $(K, \mathbf{D})$ , where K is a field of characteristic p and  $\mathbf{D} = (\mathbf{D}_1, \ldots, \mathbf{D}_e)$  is a sequence of commuting Hasse derivations on K. The field of constants<sup>2</sup> C consists of those elements of K on which all derivations  $\mathbf{D}_{i,1}$   $(i = 1, \ldots, e)$  vanish. Clearly C contains  $K^p$ .  $(K, \mathbf{D})$  is a strict  $\mathcal{D}$ -field if  $C = K^p$ .

**Definition.** Let  $L_e$  be the natural language for  $\mathcal{D}$ -fields, which contains symbols  $\{0, 1, +, -, \cdot\}$  for the field operations and unary function symbols  $D_{i,n}$  ( $i \in$ 

<sup>&</sup>lt;sup>1</sup>Equation (1.3) means that we consider only *iterative* Hasse derivations.

<sup>&</sup>lt;sup>2</sup>The definition used here differs from the definition given in [7], where the constants are killed by all  $\mathbf{D}_{i,j}$  (j > 0)

 $\{1, \ldots, e\}, n \in \mathbb{N}$ ). We denote by  $\mathrm{SCH}_{p,e}$  the  $L_e$ -theory of all separably closed, strict  $\mathcal{D}$ -fields which have degree of imperfection  $e^{3}$ .

The aim of this article is to prove the following theorem:

#### Theorem 1.1.

- 1.  $SCH_{p,e}$  is complete and has quantifier elimination.
- 2. Every  $\mathcal{D}$ -field can be extended to a model of  $SCH_{p,e}$ .
- 3. Every separably closed field of degree of imperfection e can be expanded to a model of SCH<sub>p,e</sub>.

Our theory is a variant of the theory given by M. Messmer and C. Wood in [6], where a single, non-iterative Hasse derivation was used. For e = 1 our two approaches coincide and Theorem 1.1 was proved (slightly differently) in [6].<sup>4</sup>

We will prove the theorem in Section 3. The main algebraic ingredient is the amalgamation property of the class of  $\mathcal{D}$ -fields, which we prove in Section 2, Proposition 2.6. In Section 4 we give an alternative proof for quantifier elimination.

I thank Anand Pillay for various helpful discussions.

# 2 Amalgamation

We will prove in this section that the class of  $\mathcal{D}$ -fields has the *amalgamation* property: Any two extensions of a  $\mathcal{D}$ -field K can be jointly embedded in a third extension of K.

**Lemma 2.1.** For any  $\mathcal{D}$ -field K the index of its field C of constants is bounded by  $p^e$ . Let K' be an extension of K with constant field C'. Then C' and K are linearly disjoint over C.

*Proof.* We write  $d_i$  for the derivation  $\mathbf{D}_{i,1}$  and  $C_i$  for its field of constants in K. By reordering  $\mathbf{D}$  we may assume that C is the irredundant intersection of the first f of the  $C_i$ . So the  $B_i = C_1 \cap \cdots \cap C_i$  form a properly descending sequence

$$K = B_0 \supset B_1 \supset \cdots \supset B_f = C.$$

The formula (1.3) implies that  $d_i^p = 0$  for all *i*. Since the  $d_i$  commute, each  $d_i$  maps  $B_{i-1}$  into itself. By Theorem 27.3 of [3] we find elements  $x_i \in B_{i-1}$  with  $d_i(x_i) = 1$  and for any such choice  $1, x_i, \ldots, x_i^{p-1}$  is a basis of  $B_{i-1}$  over  $B_i$ .

<sup>&</sup>lt;sup>3</sup>I.e.  $[K:K^p] = p^e$ 

<sup>&</sup>lt;sup>4</sup>M. Messmer and C. Wood have asked me to point out, that, for e > 1, there is a gap in the proof of the main theorem [6], as well as a false claim about the product rule in the non-iterative case.

Whence the  $x = x_1^{e_1} \cdots x_f^{e_f}$ ,  $(e_i < p)$  form a basis of K over  $B_f = C$ . For the same reason these elements form a basis of K' over  $B'_f \supset C'$ . Thus the x are independent over C'.

An alternative proof uses the Wronskian matrix: Let  $\theta_1, \ldots, \theta_{p^e}$  be an enumeration of all operators of the form  $\mathbf{D}_{1,n_1}\mathbf{D}_{2,n_2}\cdots\mathbf{D}_{e,n_e}$ ,  $(n_i < p)$  (or, equivalently,  $d_1^{n_1}d_2^{n_2}\cdots d_e^{n_e}$ ). It can easily be proved by a standard argument that a sequence  $x_1, \ldots, x_N$  is linearly independent over C iff the matrix  $(\theta_{\alpha}(x_{\beta}))$  has rank N (see [7, Proposition 5.1]). The Lemma follows immediately from this.

**Corollary 2.2.** Let K be a strict  $\mathcal{D}$ -field and F a  $\mathcal{D}$ -field which extends K. Then F is a separable extension of K. If  $[K : K^p] = p^e$ , F is strict iff K and F have a common p-basis.

(See [1] for the definition of p-basis and its basic properties.)

*Proof.* By the Lemma K and the field C constants of F are linearly disjoint over  $K^p$ . This implies that K and  $F^p$  are linearly disjoint over  $K^p$ . Thus F is separable over K. We have  $[K : K^p] \leq [F : C] \leq p^e$ . So, if  $[K : K^p] = p^e$ , we have  $[F : C] = p^e$ . Therefore  $C = F^p$  iff  $[F : F^p] = p^e$ , which proves the second part.

**Lemma 2.3.** Let  $(K, \mathbf{D})$  be a  $\mathcal{D}$ -field and F a field extension of K. Assume that K and F have a common p-basis. Then  $\mathbf{D}$  extends uniquely to a sequence  $\mathbf{E}$  of commuting Hasse derivations on F. Furthermore, if  $(F', \mathbf{E}')$  is an extension of  $(K, \mathbf{D})$  which contains F, the functions in  $\mathbf{E}'$  map F into itself, so that  $\mathbf{E} = \mathbf{E}' \upharpoonright F$ .

In the special case that F is a separably algebraic extension of K the Lemma is due to F.K. Schmidt ([2]) for e = 1 and to Okugawa ([7, Proposition 2.8]) for arbitrary e. We will deduce the general case from a theorem of Matsumara.

*Proof.* For a single Hasse derivation the lemma follows from the fact that field extensions with a common p-basis are 0-tale, see [3, 26.7 and 27.2]. So, if **E** is a sequence of Hasse derivations of F which extends **D**, it remains to show that the  $\mathbf{E}_i$  commute. Let us prove that  $\mathbf{E}_1$  and  $\mathbf{E}_2$  commute, i.e. that  $\mathbf{E}_{1,i}$  and  $\mathbf{E}_{2,j}$  commute for all i, j, by induction on i + j. Fix m and n and assume that  $\mathbf{E}_{1,i}$  and  $\mathbf{E}_{2,j}$  commute for all i + j < m + n. It is easy to check (use (1.2)) that then  $\mathbf{E}_{1,m}\mathbf{E}_{2,n} - \mathbf{E}_{2,n}\mathbf{E}_{1,m}$  is a derivation. Since  $\mathbf{D}_1$  and  $\mathbf{D}_2$  commute, this derivation vanishes on K and therefore also on F.

The uniqueness stated in the Lemma follows also from the following recursive formula, which shows that D can be computed from its values on a basis<sup>5</sup> of

<sup>&</sup>lt;sup>5</sup>Even the values on a p-basis would suffice.

 $F/F^p$ : Let D be any Hasse derivation. Then (2.2) below implies for r < p that

$$D_{pn+r}(x^{p}b) = \sum_{m \le n} D_{m}(x)^{p} D_{p(n-m)+r}(b).$$
(2.1)

**Lemma 2.4.** Any  $\mathcal{D}$ -field K has a smallest strict extension  $K^{\text{strict}}$ , which is a purely inseparable extension of K.

*Proof.* Consider an arbitrary Hasse derivation D. We note first that (1.2) implies

$$D_n(x^p) = \begin{cases} D_{\frac{n}{p}}(x)^p & \text{if } p|n\\ 0 & \text{otherwise} \end{cases}$$
(2.2)

Also, by (1.3), if  $D_1(x) = 0$ , we have  $D_m(x) = 0$  for all m which are not divisible by p. It follows that

$$D' = (D_0, D_p, D_{2p}, \dots)$$

is a Hasse derivation on the constant field of  $D_1$ .<sup>6</sup>

Let C be the constant field of  $(K, \mathbf{D})$ . Since the  $\mathbf{D}_i$  commute, all  $\mathbf{D}_{i,n}$  map C into itself. By the last remark  $\mathbf{D}' = (\mathbf{D}'_1, \dots, \mathbf{D}'_e)$  is a sequence of commuting Hasse derivations on C. We transport  $\mathbf{D}'$  from C to  $K^* = C^{\frac{1}{p}}$  via the Frobenius map:

$$\mathbf{D}_{i,n}^*(x) = \mathbf{D}_{pn,i}(x^p)^{\frac{1}{p}}.$$

 $\mathbf{D}^*$  extends  $\mathbf{D}$  by (2.2). We repeat this process and get an infinite sequence of purely inseparable extensions. The union of this sequence is  $K^{\text{strict}}$ .

Note that  $K^{\text{strict}}$  is separably closed if K is separably closed.

**Lemma 2.5.** Let F and L be D-fields which both extend the D-field K. Assume that, in a common field extension, F and L are linearly disjoint over K. Then FL has a unique D-structure which extends the D-structures of F and L.

*Proof.* A  $\mathcal{D}$ -module over K is a K-vector space V with a family  $\mathbf{D}_{i,n}$   $(i \in \{1, \ldots, e\}, n \in \mathbb{N})$  of commuting additive maps  $V \to V$  such that for all  $D = \mathbf{D}_i$ ,  $x \in K$  and  $v \in V$ .

$$D_0(v) = v \tag{2.3}$$

$$D_n(xv) = \sum_{a+b=n} D_a(x)D_b(v) \tag{2.4}$$

$$D_a D_b(v) = \binom{a+b}{a} D_{a+b}(v) \quad . \tag{2.5}$$

A commutative K-algebra R is a  $\mathcal{D}$ -algebra if it is a  $\mathcal{D}$ -module and the  $\mathbf{D}_i$  are Hasse derivations on R.

The following statements are easy to check (cf. [4]):

<sup>&</sup>lt;sup>6</sup>Note that  ${n \atop i} \equiv {pn \atop pi} \mod p$ .

• If V and W are  $\mathcal{D}$ -modules over K, the tensor product  $V \otimes_K W$  becomes a  $\mathcal{D}$ -module by the definition

$$\mathbf{D}_{i,n}(v \otimes w) = \sum_{a+b=n} \mathbf{D}_{i,a}(v) \otimes \mathbf{D}_{i,b}(w).$$

• If R and S are  $\mathcal{D}$ -algebras over K, their tensor product is also a  $\mathcal{D}$ -algebra.

If R and S have unit-elements, R and S are subrings of  $R \otimes_K S$ . It is clear that the  $\mathcal{D}$ -structure of  $R \otimes_K S$  is the only common extension of the  $\mathcal{D}$ -structures of R and  $S^7$ .

If F and L are linearly disjoint over D, FL is the quotient field of  $F \otimes_K L$ . By [2] and [7, Proposition 2.3] a sequence of commuting Hasse derivations on a domain extends uniquely to the quotient field. This proves the Lemma.

#### **Proposition 2.6.** The class of $\mathcal{D}$ -fields has the amalgamation property.

Proof. Let F and L be  $\mathcal{D}$ -fields which both extend the  $\mathcal{D}$ -field K. If we apply Lemma 2.3 and Lemma 2.4 to the separable algebraic closures of F and L, we see that we may assume that F and L are separably closed and strict. Then  $(K^{\text{sep}})^{\text{strict}}$  is a  $\mathcal{D}$ -subfield of F and L (again by Lemmas 2.3 and 2.4), so we may assume that K is separably closed and strict. We may also assume that F and Lare situated in a common extension field and are algebraically independent over K. By Corollary 2.2 F is a separable extension of K and therefore a regular extension, since K is separably closed. This implies that F and L are linearly independent over K and that we can extend the  $\mathcal{D}$ -structure of F and L to FL.

# 3 Proof of the Theorem

#### 1. Quantifier elimination and completeness

To prove that  $\operatorname{SCH}_{p,e}$  has quantifier elimination, we have to show that the following is true: If F and L are models of  $\operatorname{SCH}_{p,e}$  with a common substructure R, we can embed F over R in an elementary extension of L. Let K be the quotient field of R in F and K' the copy of K in L.

For all Hasse derivations D we have the recursion formula

$$D_n\left(\frac{r}{s}\right) = \frac{D_n(r) - \sum_{a < n} D_a\left(\frac{r}{s}\right) D_{n-a}(s)}{s}$$

This shows that K and K' are  $\mathcal{D}$ -subfields of F and L and are, over R, isomorphic as  $\mathcal{D}$ -fields. So we can assume that R = K.

<sup>&</sup>lt;sup>7</sup>Note that  $D_n(1) = 0$  for any Hasse derivation D and n > 0.

By amalgamation we find a  $\mathcal{D}$ -field F' which extends F and L. We may assume that F' is strict. By Corollary 2.2 F' is a separable extension of L. Since L is separably closed, we can embed F' over L in an elementary extension L' of L (see [1, Claim 2.2]). Let F'' be the copy of F' in L'.



It remains to show, that F'' is a  $\mathcal{D}$ -subfield of L' which, over L, is isomorphic to F'. But this follows immediately from Lemma 2.3, since F' and L have a common p-basis by Corollary 2.2. Note that the assumption that F is a model of  $\operatorname{SCH}_{p,e}$  was not used.

 $\operatorname{SCH}_{p,e}$  is complete since it is consistent by part 3 below and since all models contain the trivial  $\mathcal{D}$ -field  $\mathbb{F}_p$ .

#### 2. Every $\mathcal{D}$ -field is contained in a model

Let F be a  $\mathcal{D}$ -field and L be any model of  $\operatorname{SCH}_{p,e}$ . (We will see below that  $\operatorname{SCH}_{p,e}$  is consistent.). By the proof of quantifier elimination we can embed F (over  $\mathbb{F}_p$ ) in an elementary extension of L.

# 3. Every separably closed field with degree of imperfection e can be expanded to model

Let F be a separably closed field of imperfection degree e. Let  $b_1, \ldots, b_e$  be a p-basis of F. Then the  $b_i$  are algebraically independent over  $\mathbb{F}_p$  and form a pbasis of  $K = \mathbb{F}_p(b_1, \ldots, b_e)$ . Define a sequence of commuting Hasse derivations on K by

$$f(b_1, \dots, b_i + t, \dots, b_e) = \sum_{n=0}^{\infty} \mathbf{D}_{i,n}(f(b_1, \dots, b_e)) t^n.$$
 (3.1)

or, equivalently, by

$$\mathbf{D}_{i,n}(b_1^{k_1}\cdots b_e^{k_e}) = \binom{k_i}{n} b_1^{k_1}\cdots b_i^{k_i-n}\cdots b_e^{k_e}$$
(3.2)

It is easy to check, and well-known, that this definition turns K into a strict  $\mathcal{D}$ -field (see [7, Section I.1]). By Lemma 2.3 we can extend **D** to F. F is strict since  $[F:F^p] = p^e$  (Corollary 2.2). So  $(F, \mathbf{D})$  is a model of SCH<sub>p,e</sub>.

### 4 Remarks

#### Stability and elimination of imaginaries

Using the methods of [1] and [6] it is easy to prove that  $\text{SCH}_{p,e}$  is stable and has elimination of imaginaries. The stability of  $\text{SCH}_{p,e}$  can also be derived directly from the stability of separably closed fields ([8]) as follows: Let F be a separably closed field with p-basis  $b_1, \ldots, b_e$  and D a Hasse derivation of F. The formula (2.1) shows that all  $D_n$  are definable in the field F using the parameters  $D_n(b_1^{k_1}\cdots b_e^{k_e})$ .<sup>8</sup> This implies that F together with any sequence of Hasse derivations is stable.

Let me also indicate why SCH<sub>p,e</sub> has elimination of imaginaries, following [5]. One notes first, that, working in fields, it suffices to show that SCH<sub>p,e</sub> has weak elimination of imaginaries (see [5, Fact 5.5]). By a theorem of Evans, Pillay and Poizat (see [5, Proposition 5.8]) it is enough to show that every type  $q(x_1, \ldots, x_m)$  over a model  $(F, \mathbf{D})$  has a canonical base. Let  $\theta_1, \theta_2, \ldots$  be an enumeration of all operators of the form  $\mathbf{D}_{1,n_1}\mathbf{D}_{2,n_2}\cdots\mathbf{D}_{e,n_e}$ ,  $(n_i = 0, 1, \ldots)$ and let  $I_q$  be the ideal of all polynomials  $f \in F[X_{\alpha,j}]_{\alpha=1,2,\ldots;j=1,\ldots,m}$  such that the formula  $f(\theta_{\alpha}(x_j)) \doteq 0$  belongs to q. By quantifier elimination q is determined by  $I_q$ . Thus the field of definition of  $I_q$  serves as a canonical base of q.

#### Canonical *p*-bases

Let  $(F, \mathbf{D})$  be a  $\mathcal{D}$ -field with degree of imperfection e. A p-basis  $b_1, \ldots, b_e$  is canonical if for all n > 0

$$\mathbf{D}_{i,n}(b_j) = \begin{cases} 1 & \text{if } n = 1 \text{ and } i = j \\ 0 & \text{otherwise} \end{cases}.$$
 (4.1)

**Lemma 4.1.** Let F be a field with with degree of imperfection e. Every p-basis of F is a canonical p-basis of a uniquely determined sequence of commuting Hasse derivations.

*Proof.* A canonical *p*-basis  $b_1, \ldots, b_e$  determines **D** uniquely:  $\mathbf{D}_{i,n}(b_1^{k_1} \cdots b_e^{k_e})$  is given by (3.2). To compute  $\mathbf{D}_{i,n}(x)$  for arbitrary x, write

$$x = \sum_{0 \le k_1, \dots, k_e < p^m} x_{k_1 \dots k_e}^{p^m} b_1^{k_1} \cdots b_e^{k_e}$$

for some m with  $n < p^m$ . Then

$$\mathbf{D}_{i,n}(x) = \sum_{0 \le k_1, \dots, k_e < p^m} x_{k_1 \dots k_e}^{p^m} \mathbf{D}_{i,n}(b_1^{k_1} \cdots b_e^{k_e}).$$
(4.2)

Now let  $b_1, \ldots, b_e$  be any *p*-basis. The construction at the end of the last section shows that (3.2) and (4.2) define a sequence **D** of commuting Hasse derivations with canonical *p*-basis  $b_1, \ldots, b_e$ .

<sup>&</sup>lt;sup>8</sup>Actually the parameters  $b_i$  and  $D_{p^m}(b_i)$  suffice.

The **D** constructed in in the last part of the proof is strict. So we conclude, that only a strict sequence **D** can have a canonical *p*-basis. The converse is true if  $(F, \mathbf{D})$  is  $\omega$ -saturated:

**Remark.** Every  $\omega$ -saturated strict  $\mathcal{D}$ -field has a canonical p-basis.

I will give the proof only in the following special case, which will be used later.

**Corollary 4.2.** Every  $\omega$ -saturated model of SCH<sub>p,e</sub> has a canonical p-basis.

*Proof.* To have a canonical p-basis means that a certain countable set  $\Sigma(x_1, \ldots, x_e)$  of formulas is realized. Since  $\operatorname{SCH}_{p,e}$  is complete, it is enough to show that *some* model of  $\operatorname{SCH}_{p,e}$  has a canonical p-basis. For this take a separably closed field F of imperfection degree e and fix a p-basis  $\overline{b}$ . Let  $\mathbf{D}$  be the unique sequence which has  $\overline{b}$  as a canonical p-basis.  $(F, \mathbf{D})$  is a model of  $\operatorname{SCH}_{p,e}$ .

Lemma 4.1 and the last remark allow us to determine all strict sequences of commuting Hasse derivations of an  $\omega$ -saturated field F. We note first that, if  $b_1, \ldots, b_e$  is a canonical p-basis for  $\mathbf{D}$ , then  $b'_1, \ldots, b'_e$  is a canonical p-basis for  $\mathbf{D}$  iff the differences  $b_i - b'_i$  belong to

$$F^{p^{\infty}} = \bigcap_{k=1}^{\infty} F^{p^{k}} = \left\{ a \in F \mid \mathbf{D}_{i,n}(x) = 0 \ (i = 1, \dots, e; \ n = 1, 2, \dots) \right\}.$$

This gives

**Remark.** Let F be an  $\omega$ -saturated field with degree of imperfection e. There is a natural 1–1–correspondence between the set of all strict sequences of commuting Hasse derivations and the set of all p-bases modulo  $F^{p^{\infty}}$ .

#### Lambda functions

Let  $b_1, \ldots, b_e$  be a *p*-basis of *F*. The functions  $\lambda_{k_1 \ldots k_e}^m$  are defined by

$$x = \sum_{0 \le k_1, \dots, k_e < p^m} \lambda_{k_1 \dots k_e}^m (x)^{p^m} b_1^{k_1} \cdots b_e^{k_e}$$

Fix a natural number m. For a multi-index  $\kappa = (k_1, \ldots, k_e) \in \{0, \ldots, p^m - 1\}^e$ and a sequence **D** of Hasse derivations let us use the notations

$$b^{\kappa} = b_1^{k_1} \cdots b_e^{k_e}$$
 and  $\mathbf{D}_{\kappa} = \mathbf{D}_{1,k_1} \mathbf{D}_{2,k_2} \cdots \mathbf{D}_{e,k_e}$ .

If we apply  $\mathbf{D}_{\kappa}$  to the equation

$$x = \sum_{\mu} \lambda^m_{\mu}(x)^{p^m} b^{\mu},$$

we obtain

$$\mathbf{D}_{\kappa}(x) = \sum_{\mu} \lambda_{\mu}^{m}(x)^{p^{m}} \mathbf{D}_{\kappa}(b^{\mu})$$

If **D** is strict, the Wronski matrix  $(\mathbf{D}_{\kappa}(b^{\mu}))$  is always regular. If  $b_1, \ldots, b_e$  is canonical for **D**, its entries are, up to factors from  $\mathbb{F}_p$ , monomials in the  $b_i$ . It is also easy to see that the determinant is 1. This yields

**Lemma 4.3.** Let  $(F, \mathbf{D})$  be a  $\mathcal{D}$ -field with canonical *p*-basis  $b_1, \ldots, b_e$ . Then the functions  $(\lambda_{\mu}^m(x))^{p^m}$  are polynomials in  $b_1, \ldots, b_e$  and the  $\mathbf{D}_{\kappa}(x)$ .  $\Box$ 

#### Quantifier elimination

Let  $T_{p,e}$  denote the theory of separably closed fields F of characteristic p with a named p-basis  $b_1, \ldots, b_e$ . It is shown in [1] that  $T_{p,e}$  is complete and has quantifier elimination if one adds function symbols for the  $\lambda_{\mu}^m$  to the language.<sup>9</sup>

This fact can be used to give an alternative proof for the quantifier elimination of  $\operatorname{SCH}_{p,e}$ : Let  $\phi(\bar{x})$  be an  $L_e$ -formula and  $(F, \mathbf{D})$  a saturated model of  $\operatorname{SCH}_{p,e}$ . By Corollary 4.2 we can find a canonical *p*-basis  $b_1, \ldots, b_e$ . Since we can define the  $\mathbf{D}_{i,n}$  in  $(F, b_1, \ldots, b_e)$ ,  $\phi(\bar{x})$  is equivalent to a Boolean combination of polynomial equations between  $b_1, \ldots, b_e$  and terms of the form  $\lambda_{\mu}^m(x_i)$ , for sufficiently large *m*. By taking  $p^m$ -th powers we can replace the  $\lambda_{\mu}^m(x_i)$  by  $\lambda_{\mu}^m(x_i)^{p^m}$ . By the last lemma we obtain an equivalent Boolean combination of equations of the form

$$\sum_{\kappa} q_{\kappa}(\bar{x}) \, b^{\kappa} \doteq 0 \tag{4.3}$$

where the  $q_{\kappa}(\bar{x})$  are terms in the  $\mathbf{D}_{\kappa}(x_i)$ . The equivalence holds for any choice of the canonical *p*-basis  $b_1, \ldots, b_e$ . Since  $F^{p^{\infty}}$  is infinite, we can find the  $b_1, \ldots, b_e$ algebraically independent over any given tuple  $\bar{x}$ . This shows that we can replace each equation (4.3) by  $\bigwedge_{\kappa} q_{\kappa}(\bar{x}) \doteq 0$ . We observe finally that the resulting quantifier free  $L_e$ -formula does not depend on the choice of F.

## References

- Françoise Delon. Separably closed fields. In Bouscaren, editor, Model theory and algebraic geometry: An Introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture, volume 1696 of Lecture Notes in Mathematics, pages 143–176. Springer, Berlin, 1998.
- [2] Helmut Hasse and F.K. Schmidt. Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper mit einer Unbestimmten. J. Reine Angew. Math., 177:215–237, 1937.

<sup>&</sup>lt;sup>9</sup>Only the  $\lambda^1_{\mu}$  are needed for quantifier elimination. As Françoise Delon has explained to me, also the constants for the *p*-basis can be disposed of.

- [3] Hideyuki Matsumara. Commutative ring theory. Cambridge University Press, 1986.
- [4] B. Heinrich Matzat. Differential galois theory in positive characteristic. Lecture Notes, October 2001.
- [5] Margit Messmer. Some model theory of separably closed fields. In D. Marker, M. Messmer, and A. Pillay, editors, *Model Theory of Fields*, volume 5 of *Lectures Notes in Logic*, pages 135–152. Springer, Berlin, 1996.
- [6] Margit Messmer and Carol Wood. Separably closed fields with higher derivation I. The Journal of Symbolic Logic, 60(3):898–910, September 1995.
- [7] K. Okugawa. Basic properties of differential fields of arbitrary characteristic and the Picard–Vessiot theory. J. Math. Kyoto Univ., 2(3):294–322, 1963.
- [8] Carol Wood. Notes on the stability of separably closed fields. J. Symbolic Logic, 44(3):412–416, September 1979.

MATHEMATISCHES INSTITUT ECKERSTRASSE 1 79104 FREIBURG, GERMANY

ziegler@uni-freiburg.de